UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/635,015	08/04/2003	Christopher L. Hamlin	03-0340	7590

24319	7590	09/21/2007

LSI CORPORATION
1621 BARBER LANE
MS: D-106
MILPITAS, CA 95035

EXAMINER
KHOSHNOODI, NADIA

ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
09/21/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

		Application No.	Applicant(s)
Office Action Summary		10/635,015	HAMLIN, CHRISTOPHER L.
		Examiner	Art Unit	
		Nadia Khoshnoodi	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>25 June 2007</u>.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-22</u> is/are pending in the application.

    4a) Of the above claim(s) <u>23-31</u> is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-22</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>04 August 2003</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date <u>2/7-19-2004</u>.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Response to Election/Restrictions Remarks

Claim 23-31 are withdrawn from further consideration pursuant to 37 CFR 1.142(b), as being drawn to a nonelected invention, there being no allowable generic or linking claim. Applicant timely traversed the restriction (election) requirement in the reply filed on 6/25/2007.

Applicant's election with traverse of Group 1 (claims 1-22) in the reply filed on 6/25/2007 is acknowledged. The traversal is on the ground(s) that Applicants contend that examination of claims 1-31 would pose no serious burden on the Examiner, and additionally that Applicants should not be forced to divide the invention among multiple applications. This is not found persuasive because Examiner has shown, as set forth in the previous Office Action detailing the restriction requirement, that the inventions were broken up into two groups due to the fact that the two inventions would require a separate search for each in two different subclasses. These two subcombinations usable together do not overlap in scope and are not obvious variants, since Group 2 has separate utility such as determining if an intrusion has occurred based on observing whether or not the mode of operation has changed (See MPEP 806.05(d)).

The requirement is still deemed proper and is therefore made FINAL.

Claim Rejections - 35 USC § 101

I.   35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

II.   Claims 1-22 are rejected under 35 U.S.C. 101 because the claimed invention produces no tangible result to form the basis of statutory subject matter under 35 U.S.C. 101. The claims are not a practical application of an abstract idea. The result of these claims is not in a tangible form. Rather, they are abstract results since one element, namely the trusted authority, only controls operation of another element, namely the buried nucleus. Merely controlling operation of another entity without claiming what the results of this controlling step are, is not tied and does not correspond to the real world, i.e. the results are left to an abstract idea. Furthermore, claim 10 has been defined as being equipped to accept a key when using the secure protocol, where this claim does not recite actually performing that step. Applicants may choose to amend claims 9 and 10 to include a step which shows the end result of the controlling operation. Also, in order to meet the "useful" requirement, there must be some application implemented based on the end result.

Claim Rejections - 35 USC § 102

III.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this

subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

IV.   Claims 1-9 are rejected under 35 U.S.C. 102(e) as being fully anticipated by Elazar et al., US Pub. No. 2004/0039932.

As per claim 1:

Elazar et al. teach a distributed architecture of an information handling system, comprising: a buried nucleus inaccessible for inspection without heroic means while said buried nucleus is in operation (par. 26 and par. 30); and a trusted authority for generating a secure protocol, said secure protocol controlling operation of said buried nucleus (par. 33).

As per claim 2:

Elazar et al. teach the distributed architecture of claim 1. Furthermore, Elazar et al. teach wherein said buried nucleus includes at least one LFSR (linear feedback shift register) (par. 25).

As per claim 3:

Elazar et al. teach the distributed architecture of claim 1. Furthermore, Elazar teach wherein said buried nucleus includes at least one reconfigurable core (par. 27).

As per claim 4:

Elazar et al. teach the distributed architecture of claim 1. Furthermore, Elazar et al. teach wherein said buried nucleus includes at least one programmable logic block (par. 27).

As per claim 5:

Elazar et al. teach the distributed architecture of claim 1. Furthermore, Elazar et al. teach wherein said buried nucleus includes at least one non-volatile RAM (par. 27).

As per claim 6:

Elazar et al. teach the distributed architecture of claim 1. Furthermore, Elazar et al. teach wherein said buried nucleus includes at least one matrix multiplier (par. 34).

As per claim 7:

Elazar et al. teach the distributed architecture of claim 1. Furthermore, Elazar et al. teach wherein said trusted authority is a back-end secure server (par. 33).

As per claim 8:

Elazar et al. teach the distributed architecture of claim 1. Furthermore, Elazar et al. teach wherein said trusted authority is a cell phone operator with a trusted command and control center (par. 29).

As per claim 9:

Elazar et al. teach the distributed architecture of claim 1. Furthermore, Elazar et al. teach wherein said trusted authority is an encrypted medium (par. 33).

Claim Rejections - 35 USC § 103

V.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

VI.   Claims 10-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Elazar et al., US Pub. No. 2004/0039932, and further in view of Parks et al., US Patent No. 7,146,504.

As per claim 10:

Elazar et al. substantially teach a distributed architecture of an information handling system, comprising: (a) a hardware/software system, comprising: a microchip including an outer region having I/O pins and a buried nucleus inaccessible for inspection without heroic means when said buried nucleus is in operation (par. 26 and par. 30); and external software connected to said I/O pins for controlling said I/O pins (par. 25); and (b) a trusted authority for generating a secure protocol, said secure protocol controlling operation of said hardware/software system (par. 36); (c) wherein said buried nucleus is equipped to accept a key delivered through said secure protocol (par. 35, lines 15-16).

Not explicitly disclosed is wherein the buried nucleus is equipped to decipher an encrypted key delivered through said secure protocol. However, Parks et al. teach that a trusted authority which supplies the protected digital content, may also encrypt the key used to encrypt the digital content. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Elazar et al. to encrypt the content key where the DRM component, i.e. buried nucleus, can decrypt the content key when it is delivered through a secure protocol. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Parks et al. suggest that sending the content key in encrypted form secures the key so that only that specific user device can obtain access to the digital content the user is authorized to access in col. 4, lines 50-61.

As per claim 11:

Elazar et al. and Parks et al. substantially teach the distributed architecture of claim 10. Furthermore, Elazar et al. teach wherein said buried nucleus includes at least one LFSR (linear

feedback shift register) (par. 25).

As per claim 12:

Elazar et al. and Parks et al. substantially teach the distributed architecture of claim 10.

Furthermore, Elazar et al. teach wherein said buried nucleus includes at least one reconfigurable

core (par. 27).

As per claim 13:

Elazar et al. and Parks et al. substantially teach the distributed architecture of claim 10.

Furthermore, Elazar et al. teach wherein said buried nucleus includes at least one programmable

logic block (par. 27).

As per claim 14:

Elazar et al. and Parks et al. substantially teach the distributed architecture of claim 10.

Furthermore, Elazar et al. teach wherein said buried nucleus includes at least one non-volatile

RAM (par. 27).

As per claim 15:

Elazar et al. and Parks et al. substantially teach the distributed architecture of claim 10.

Furthermore, Elazar et al. teach wherein said buried nucleus includes at least one matrix

multiplier (par. 34).

As per claim 16:

Elazar et al. and Parks et al. substantially teach the distributed architecture of claim 10.

Not explicitly disclosed is wherein said encrypted key is encrypted with digital watermarking.

However, Elazar et al. teach encrypting the actual content by adding overlay information.

Therefore, it would have been obvious to a person in the art at the time the invention was made

to modify the method disclosed in Elazar et al. to also use digital watermarking to encrypt the key. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Elazar et al. suggest there are several possible ways to encrypt a document which may be used in order to secure and verify the contents which are encrypted in par. 36, lines 5-20.

As per claim 17:

Elazar et al. and Parks et al. substantially teach the distributed architecture of claim 10. Not explicitly disclosed is wherein said encrypted key is encrypted with a fast elliptical algorithm. However, Elazar et al. teach encrypting the actual content with a fast elliptical algorithm. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Elazar et al. to also use a fast elliptical algorithm to encrypt the key. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Elazar et al. suggest there are several possible encryption algorithms which may be used in order to secure the contents being encrypted in par. 35.

As per claim 18:

Elazar et al. and Parks et al. substantially teach the distributed architecture of claim 10. Not explicitly disclosed is wherein said encrypted key is encrypted with Triple DES. However, Elazar et al. teach encrypting the actual content with Triple DES. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Elazar et al. to also use a Triple DES to encrypt the key. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made,

would have been motivated to do so since Elazar et al. suggest there are several possible

encryption algorithms which may be used in order to secure the contents being encrypted in par.

35.

As per claim 19:

Elazar et al. and Parks et al. substantially teach the distributed architecture of claim 10.

Not explicitly disclosed is wherein said encrypted key is encrypted with a Rijndael algorithm.

However, Elazar et al. teach encrypting the actual content with AES. Therefore, it would have

been obvious to a person in the art at the time the invention was made to modify the method

disclosed in Elazar et al. to also use a Rijndael algorithm to encrypt the key. This modification

would have been obvious because a person having ordinary skill in the art, at the time the

invention was made, would have been motivated to do so since Elazar et al. suggest there are

several possible encryption algorithms which may be used in order to secure the contents being

encrypted in par. 35.

As per claim 20:

Elazar et al. and Parks et al. substantially teach the distributed architecture of claim 10.

Furthermore, Elazar et al. teach wherein said trusted authority is a back-end secure server (par.

33).

As per claim 21:

Elazar et al. and Parks et al. substantially teach the distributed architecture of claim 10.

Furthermore, Elazar et al. teach wherein said trusted authority is a cell phone operator with a

trusted command and control center (par. 29).

As per claim 22:

Elazar et al. and Parks et al. substantially teach the distributed architecture of claim 10.

Furthermore, Elazar et al. teach wherein said trusted authority is an encrypted medium (par. 33).

References Cited, Not Used

The prior art made of record and not relied upon is considered pertinent to applicant's

disclosure.

1. US Patent No. 6,449,367
2. US Pub. No. 2003/0226012
3. US Pub. No. 2003/0007646,
4. US Pub. No. 2004/0054894
5. US Pub. No. 2003/0191942
6. US Pub. No. 2004/0064714

The above references have been cited because they are relevant due to the manner in which the

invention has been claimed.

Conclusion

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825.

The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the

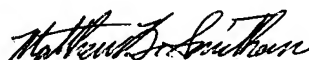organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would

like assistance from a USPTO Customer Service Representative or access to the automated

information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Nadia Khoshnoodi
Examiner
Art Unit 2137
9/14/2007

NK

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137